REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-25 are pending in the application. The Examiner additionally stated that claims 1-25 are rejected. By this communication, claims 1-3, 9, 12-14, 16, and 21 are amended. Hence, claims 1-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Amendment

The Examiner objected to the amendment filed 27 April 2009 under 35 U.S.C. 132(a) because it introduced new matter into the disclosure. The Examiner noted that the added material not supported by the original disclosure is as follows: single atomic cryptographic instruction.

Applicant respectfully traverses the objection and notes that numerous paragraphs and drawings in the original disclosure provide support for "single atomic cryptographic instruction. For instance, in paragraph [0020], the present inventors note a need for "dedicated cryptographic hardware within a present day microprocessor such that an application program that requires a cryptographic operation can direct the microprocessor to perform the cryptographic operation via a *single, atomic, cryptographic instruction*."

In addition, paragraph [0028] references FIGURE 4 that depicts "an embodiment of *an atomic cryptographic instruction* according to the present invention."

Paragraph [0043] introduces the present invention where a "cryptographic unit is activated to perform cryptographic operations via programming of a *single cryptographic instruction*."

In paragraph [0045], the present inventors disclose "an application program that requires the prescribed cryptographic operation can direct the microprocessor 301 to perform the operation via *a single cryptographic instruction* 322."

Furthermore, paragraph [0049] introduces FIGURE 4, where a "a block diagram is provided showing one embodiment of *an atomic cryptographic instruction* 400 according to the present invention.

Moreover, paragraph [0052] introduces FIGURE 5, where a table is presented "illustrating exemplary block cipher mode field values according to *the atomic cryptographic instruction* of FIGURE 4."

The above excepts from the instant disclosure are only a few of the many references made therein that sufficiently support references to a single atomic cryptographic instruction. Consequently, it is respectfully requested that the objection be withdrawn.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-25 under 35 U.S.C. 103(a) as being unpatentable over Kessler, US6789147 (hereinafter, "Kessler"), in view of Colavin, U.S. Publication No. 20040103263 (hereinafter, "Colavin"), and further in view of Miller, US6081884 (hereinafter, "Miller"). Applicant respectfully traverses the Examiner's rejections.

Claim 1 recites:

1. An apparatus for performing cryptographic operations, comprising:

an x86-compabitle microprocessor, comprising:

fetch logic, configured to receive a single, atomic cryptographic instruction, wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation, and wherein said single, atomic cryptographic instruction prescribes one of a plurality of cryptographic algorithms;

algorithm logic, operatively coupled to said single, atomic cryptographic instruction, configured to direct said x86-compatible microprocessor to execute said encryption operation according to said one of a plurality of cryptographic algorithms; and

execution logic, operatively coupled to said algorithm logic, configured to execute said one of the cryptographic operations, wherein said execution logic comprises a cryptography unit for executing a plurality of cryptographic rounds required to complete said encryption operation.

The Examiner asserted that the term "single atomic cryptographic instruction is undefined by the specification, and therefore the cryptographic instructions of Kessler meet the claims instructions using a broad but reasonable interpretation of the specification.

In reply, Applicant respectfully asserts that the specification indeed specifically defines the term "single atomic cryptographic instruction," as is evidenced by citation of the numerous paragraphs above. Furthermore, one embodiment of the single atomic cryptographic instruction according to the present invention is depicted in FIGURE 4 in detail and is discussed in associated specification paragraphs. Moreover, as will be argued hereinbelow, the single atomic cryptographic instruction according to the present invention is patently distinct from and nonobvious over the cited references.

Nowhere do the cited references disclose **a single, atomic cryptographic instruction, wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation**, as is recited in claim 1.

The Examiner argued that because Miller teaches that the x86 instruction set has been widely accepted because of its compatibility with a large amount of software, it would have been obvious to one of ordinary skill in the art at the time of invention for the co-processor described in Kessler to implement the x86 instruction set. Applicant respectfully disagrees with these points because nowhere do these references suggest that use of an x86-compatible microprocessor for purposes of performing an encryption operation. Applicant submits that Kessler teaches a security co-processor interface, for performing security operations. Such an interface does not constitute the functions that are commensurate with implementation of the x86 instruction set, which would yield an x86-compatible microprocessor, as is disclosed in the instant specification. Applicant respectfully asserts that an x86-compatible microprocessor is a well-known term of art and is sufficiently supported within the instant disclosure to include, as Miller discloses "compatibility with a large amount of software," among other features. Thus, it does not follow that one skilled would be even remotely motivated to implement the x86 instruction set on the co-processor of Kessler for Kessler's co-processor only possesses those capabilities needed to perform security operations.

In addition, Applicant submits that it is difficult to find any practical combination of Kesseler, Colavin, and Miller, which would result in the limitation cited above. The only contribution that Miller makes to the argument is that the x86 instruction set is well-known and widely accepted. Applicant concedes this point. However, that the x86 instruction set is well-known and widely accepted does not provide sufficient motivation to add an estimated two orders of magnitude of functionality to a security co-processor interface in order to produce an x86-compatible microprocessor.

Furthermore, Applicant respectfully submits that Colavin does not practically add any support to the argument other than the fact that an encryption is mentioned in paragraph [0002] as one example of a program that has high instruction level parallelism and that VLIW and superscalar architectures support concurrent execution of instructions. The point that Colavin makes in the Abstract and paragraph [0018] is that identical processing elements in a coprocessor configured in parallel can be used to accelerate execution of portions of a program having high instruction level parallelism. Applicant is respectfully unclear as to the Examiner's motivation in providing the Colavin citations because the Examiner argues that Kessler does not specify that the co-processor executes that program that includes the cryptographic operations, but that addition of Colavin meets the limitation that the "single atomic instruction is one of the instructions in an application program, wherein said application is executed by said microprocessor to obtain expected results." This is not what is recited in claim 1, but rather "wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation." If the Examiner is suggesting that Colavin's co-processor executes portions of an application program, then Applicant agrees with this point, but like the citation of Miller, Applicant argues that such a combination does not have any practical relevance.

Applicant has thoroughly studied the teachings of Kessler, Colavin, and Miller, both alone and in combination, and finds that Kessler and Colavin fail to teach any form of **an x86-compatible microprocessor**, as is recited in claim 1. As has been previously submitted, Kessler teaches a security co-processor interface. Colavin teaches clustered VLIW processing elements, coupled by a runtime reconfigurable inter-cluster interconnect to form a coprocessor executing only those portions of a program having high instruction level parallelism. (Abstract). And Miller only adds that the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software. The combination of these three references do not yield anything practical for one skilled in the microprocessor arts. Furthermore, the combination of these references fail to suggest **an x86-compatible microprocessor** that comprises, *inter alia*, **a single, atomic cryptographic instruction, wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation**, as is recited in claim 1.

Thus, for at least the above reasons, it is respectfully asserted that claim 1 is patentably distinct and non-obvious over the cited art. Consequently, it is requested that the rejection be withdrawn.

Claim 21 recites substantially the same limitations as have been argued above as being allowable over the combination of Kessler, Colavin, and Miller. Accordingly, it is requested that the rejection of claim 21 be withdrawn as well.

With respect to claims 2-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-15.

With respect to claims 22-25, these claims depend from claim 21 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 22-25.

As per claim 16, substantially the same limitations are recited as have been argued above with regard to claims 1 and 21, the exception being that claim 16 recites that the single atomic cryptographic instruction prescribes a decryption operation. Consequently, it is requested that the rejection be withdrawn since the recited limitations are not taught, contemplated, or suggested by the combination of Kessler, Colavin, and Miller.

With respect to claims 17-20, these claims depend from claim 16 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler, Colavin, and Miller. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 16-20.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/
By: ______________________

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

10/25/2009
Date: ______________________